AF

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Cameron Mashayekhi

Title: APPARATUS AND METHOD FOR AUTOMATICALLY AUTHENTICATING A NETWORK CLIENT

Docket No.: 1565.027US1
Filed: March 3, 2000
Examiner: Matthew E. Heneghan

Serial No.: 09/518,664
Due Date: November 11, 2006 (Sat.)
Group Art Unit: 2134

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

We are transmitting herewith the following attached items (as indicated with an "X"):

X Response to Notice of Non-Compliant Appeal Brief (5 pgs.).
X Return postcard.

If not provided for in a separate paper filed herewith, Please consider this a PETITION FOR EXTENSION OF TIME for sufficient number of months to enter these papers and please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
Customer Number 21186

By: /Joseph P. Mehrle/
Atty: Joseph P. Mehrle
Reg. No. 45,535

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: MS Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 13 day of November, 2006.

Peter Rebuffoni
Name

Peter Rebuffoni
Signature

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Cameron Mashayekhi	Examiner: Matthew Heneghan
Serial No.:	09/518,664	Group Art Unit: 2134
Filed:	March 3, 2000	Docket: 1565.027US1
Title:	APPARATUS AND METHOD FOR AUTOMATICALLY AUTHENTICATING A NETWORK CLIENT	

RESPONSE TO NOTICE OF NON-COMPLIANT APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

This responds to the Notice of Non-Compliant Appeal Brief mailed on October 11, 2006. In compliance with MPEP 1205.03(B) and 37 CFR 41.37(c)(1)(v), Appellants submit the following corrected section from Appellants' previously-submitted Appeal Brief filed September 27, 2006.

Appellant's attorney would like to note that the additions to the attached corrected section were made after conferring with the U.S. Patent Office by telephone. Appellant's attorney was told that the best way to address the Notice of Non-Compliant Appeal Brief was to identify in ALL CAPS and in **Bold** the independent claim that each paragraph in the Summary of the Claimed Subject Matter is referring.

Please replace the previously submitted Summary of Claimed Subject Matter Section 5 with the below replacement.

5. SUMMARY OF CLAIMED SUBJECT MATTER

Some aspects of the present inventive subject matter include, but are not limited to, systems and methods for automatically authenticating a network client.

CLAIM 1

In an aspect of the invention, an authentication system suitable for automatically providing authentication to a user at a client node is presented (FIG. 2 and Specification, page 3 first full paragraph, page 7 first full paragraph and continuing through at least the first full paragraph of page 8). The user provides a user secret (Specification, page 5 second paragraph lines 19-20) and requests access to network resources resident at one or more server nodes in a distributed network system (Specification, page 7 lines 1-3). The authentication system includes: a local application program interface for receiving the user secret, where the local application program interface is in communication with a requested network resource and the client node (FIG. 2 reference numeral 121 and Specification page 8 lines 17-21). The authentication system also includes a cryptography service node having means for providing a common key and algorithm, and having means for providing a client/server session key and algorithm, where the session key is associated with a single session during a single logon of the user and if the session terminates the session key becomes invalid (FIG. 2 reference numeral 125 and Specification page 9 lines 6-12 and page 13 lines 13-20). The authentication system also includes an authentication database in communication with the local application program interface and with the cryptography service node (FIG. 2 reference numeral 103; FIG. 3; and Specification page 8 lines 10-13). The authentication database includes an authentication secret associated with the user (Specification page 8 lines 10-13); means for encrypting the authentication secret using the common key and algorithm (FIG. 7B blocks 347 and 349 and Specification page 16 lines 22-27); and means for encrypting the common key using the client/server session key and algorithm

(FIG. 7B blocks 347 and 349 and Specification page 16 lines 22-27). The local application program interface sends an encrypted authentication secret, an encrypted common key, and the session key to the client node for use with the requested network resource, and the common key is a shared and same key, and the use occurs during the single session of the user and expires when the single session expires (FIG. 8B, Specification page 18 lines 3-12 and Specification page 13 lines 13-20).

CLAIM 9

According to another aspect, a method for automatically authenticating a user at a network client node in a distributed network system in response to a user request for access to network resources resident in one or more server nodes is provided (FIGS. 6A-6C and Specification page 12 lines 20-29). A network resource identifier, a network resource policy, and an authentication secret to an authentication database, are provided; the network resource identifier is associated with the requested network resource (FIG. 6A reference block 311 and Specification page 13 lines 21-28). Further, the authentication secret is retrieved in response to the user request, and the authentication secret is associated with the user and with the network resource identifier (FIG. 6C and Specification page 14 lines 19-28). The authentication secret is encrypted with a common key and algorithm (FIG. 7B blocks 347 and 349 and Specification page 16 lines 22-27). The common key is a shared and same key (Specification page 17 lines 3-18). Also, the common key and algorithm are encrypted with a client/server session key and algorithm (FIG. 7B blocks 347 and 349 and Specification page 16 lines 22-27). The session key is associated with a single a session of a logon of the user and when the session terminates the session key becomes invalid (Specification page 13 lines 13-20). Moreover, the encrypted authentication secret and the common key are sent to the client node for use by the client during the single session, and the use expires when the single session expires (Specification page 13 lines 13-20).

CLAIM 15

In still another aspect, a method for authenticating a client to a network resource is presented (FIGS. 6A-6C and 7A-7C). A client receives a request for a network resource and the

client is authenticated and a secure session is created (Specification page 9 lines 10-12; Specification page 13 lines 17-20; Specification page 14 lines 23-25; FIG. 6C reference block 325). An authentication secret is created for access to the network resource (FIG. 9B reference block 407 and Specification page 18 line 30 through page 19 line 5. Further, the authentication secret is encrypted within a common key, where the common key is a shared and same key (FIG. 7B blocks 347 and 349 and Specification page 16 lines 22-27; Specification page 17 lines 3-18). Moreover, the common key is encrypted with a session key associated with the secure session, where the session key becomes invalid when the secure session terminates and where the secure session is associated with a single login session of the client (FIG. 7B blocks 347 and 349 and Specification page 16 lines 22-27; Specification page 13 lines 13-20). Furthermore, the encrypted common key, the encrypted authentication secret, and the session key are is transmitted to the client for use in accessing the network resource during the single login session, and the use expires when the single login session expires (Specification page 13 lines 13-20).

This summary does not provide an exhaustive or exclusive view of the present subject matter, and Appellant refers to the appended claims and its legal equivalents for a complete statement of the invention

CONCLUSION

In accordance with MPEP 1205.03(B) and 37 CFR 41.37(c)(1)(v), only the non-compliant section of Appellant's previously-submitted Appeal Brief has been included in this response.

Appellant respectfully submits that the Examiner withdraw the non-compliant status and examine the Appeal Brief.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

CAMERON MASHAYEKHI

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(513) 942-0224

Date November 13, 2006 By /Joseph P. Mehrle/

Joseph P Mehrle
Reg. No. 45,535

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: MS Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this 13 day of November 2006.

Peter Rebuffoni
Name

Signature